REMARKS

Claims 1 - 21 are presently pending in the application. Claims 1, 8 and 15 have been amended. No new matter has been added and support for the amendments to the claims can be found in the specification and drawings. The specification has been amended to delete the embedded hyperlinks in response to the Examiner's objection. In view of the above claim amendments and arguments for patentability presented hereinbelow, Applicants respectfully submit that these claims are now in condition for allowance.

Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-21 stand rejected under Section 103(a) as being unpatentable over Peyret, et al. U.S. Patent No. 5,923,884 ("Peyret"). Applicants respectfully traverse this rejection and submit that Peyret fails to disclose or suggest the claimed invention.

In accordance with an aspect of the present invention, a methodology is provided for reducing the risk of misuse of a user's credit card number while avoiding having to securely contact and authenticate with a card issuer before each transaction in an "online" manner. A protocol is provided for generating "tokens" (i.e., a special packet that contains data) that may be used in lieu of a conventional account number and which reflect transaction restrictions that must be satisfied for the transaction to be approved. The account number is assumed to be a shared secret between the card issuer and the card holder. The tokens, in accordance with an embodiment of the invention, have a length and format identical to the account number, thereby allowing easy layering of the protocol on existing commerce infrastructures. In accordance with an aspect of the invention, an account number such as a credit card number or a calling card number is converted into a symmetric cryptographic key, for example by using a cryptographic hash function. The transaction restrictions are encoded into information that is encrypted using the symmetric cryptographic key to obtain a token which may be utilized in the transaction and verified by a card issuer using the account number. In one embodiment of the invention, the tokens are generated

by a program executing on a computing device. In accordance with another aspect of the invention, a card issuer receives the token and information identifying the account from a merchant requesting authorization for a transaction. The card issuer decrypts the token using a symmetric cryptographic key converted from the account number associated with the account with the card issuer. The card issuer can then verify information retrieved from the token and approve the transaction if the transaction satisfies any restrictions retrieved from the token. Thus, the tokens have functionality limited by the card holder and can be generated in an "off-line" manner without requiring any interaction with the card issuer. See specification at ¶0004.

Representative claim 1, as amended, calls for a method for facilitating transactions, comprising the steps of:

> receiving from a merchant, desiring to receive authorization for a transaction, *a token comprising a special packet that contains data that can be used in place of a credit card number* and information identifying an account with a card issuer;
>
> *decrypting the token* using a symmetric cryptographic key converted from an account number associated with the account with the card issuer; and
>
> verifying information retrieved from the token and approving the transaction if the transaction satisfies any restrictions retrieved from the token. Emphasis added.

The Examiner contends, with regard to independent claims 1, 8 and 15, that "Peyret discloses smart cards that are themselves tokens, smart cards that are also phone cards, usage rights, preset values, and other restrictions on the smart card, inherently the smart card transaction itself, including the merchant, card issuer, and card user, and public key encryption i.e. PKI and HASH functions (see at least column 1, lines 507 [sic]; column 1, lines 33-52; column 5, lines 30-35)." Office Action at page 3. Applicants respectfully submit that this contention is wholly without merit. The present invention has nothing to do with smart cards. Claims 1, 8 and 15 have been amended to clarify what is meant by a "token" in the context of the present invention. In particular, the token comprises *"a special*

packet that contains data that can be used in place of a credit card number." In this regard, a protocol is provided for generating tokens that may be used in lieu of a conventional account number and which reflect transaction restrictions that must be satisfied for the transaction to be approved. Peyret is devoid of any teaching, suggestion or mention of tokens used in this manner. By way of contrast, Peyret discloses:

> *...a smart card, as well as a system and method for loading applications into the memory of a smart card which may load any type of application and its associated use rights, wherein the use rights may have any type of units.* In addition, the system may load one or more disposable applications onto a permanent smart card since those disposable applications, once depleted, may be replaced with a new applet.
>
> The invention also provides an applet loading system for a smart card wherein the use rights associated with an applet may be replenished by reloading the applet and the use rights into the memory of the smart card. The system for loading applications into a smart card may be universal so that a single loading system may be used for a variety of applications. In accordance with the invention, a system and method for reloading applications within a smart card is provided wherein the system may have a storage, remotely from said smart card, that stores an applet and use rights with a predetermined initial value, associated with the applet, and has a smart card having a processing unit, and a memory unit, the memory unit being connected to the processing unit and storing a second application having use rights. The smart card may be connected to said remote storage means, and the application, having use rights with a predetermined value, may be loaded from said remote storage means into said smart card. A smart card is also provided having a processor for executing an application, a memory, connected to the processor, for storing multiple applications, including a first application having first use rights and having first values associated with the first use rights, the first value changing from a predetermined initial value with use of the first use rights, a system for loading in the smart card a second application from a remote location over an interface, the second application having second use rights, a system for storing said second application into said memory in said smart card, and a system for changing the use rights of said first application and said second application. A method of replenishing the use rights in a smart card is also provided. Col. 3, line 46 – Col. 4, line 16 (emphasis added).

....

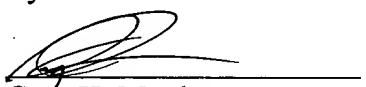
FIG. 1 is a block diagram of a smart card 20, also known as *a token*, of the type with which the invention may be employed. Col. 4, lines 53 – 55 (emphasis added).

In view of the foregoing, Peyret fails to fails to disclose or suggest any of the steps set forth in representative claim 1. Peyret's "token" is defined in a completely different context. Specifically, there is nothing in Peyret that suggests the step of "receiving from a merchant, desiring to receive authorization for a transaction, *a token comprising a special packet that contains data that can be used in place of a credit card number* and information identifying an account with a card issuer." Peyret simply discloses a smart card having use rights stored in memory, where the use rights are associated with an applet and may be replenished by reloading an applet and the use rights into the memory of the card. There is nothing in this reference that refers to using a token to transfer credit card information transparently in the manner claimed by Applicants. Likewise, Peyret fails to disclose or suggest the additional steps of "*decrypting the token* using a symmetric cryptographic key converted from an account number associated with the account with the card issuer; and verifying information retrieved from the token and approving the transaction if the transaction satisfies any restrictions retrieved from the token." The fact that Peyret discloses PKI and HASH functions as asserted by the Examiner is immaterial. Peyret simply teaches that authentication and validation of incoming requests *to change the use rights stored in memory on the smart card* "may be conducted using cryptographic systems, such as public key encryption, or any other security system." See Col. 5, lines 27 – 35. This has no applicability to the present invention. Accordingly, it is respectfully submitted that independent claim 1 and those claims dependent on claim 1, are patentable over Peyret. It is further submitted that independent claims 8 and 15 which contains similar limitations, as well as those claims dependent thereon, are patentable over Peyret for the same reasons set forth above.

In view of the foregoing, Applicants respectfully submit that claims 1 – 21 are patentable over the cited art and allowance of these claims at an early date is solicited.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C.F.R. 1.16 or 1.17 to AT&T Corp. Account No. 01-2745. The Examiner is invited to contact the undersigned at (201) 224-7957 to discuss any matter concerning this application.

Respectfully submitted,
Aviel D. Rubin, et al.
By:



Date: 2/10/05

Gary H. Monka
Registration No. 35,290
Attorney for Applicant

Canavan & Monka, LLC.
805 Partridge Drive
Bridgewater, New Jersey 08807
(201) 224-7957